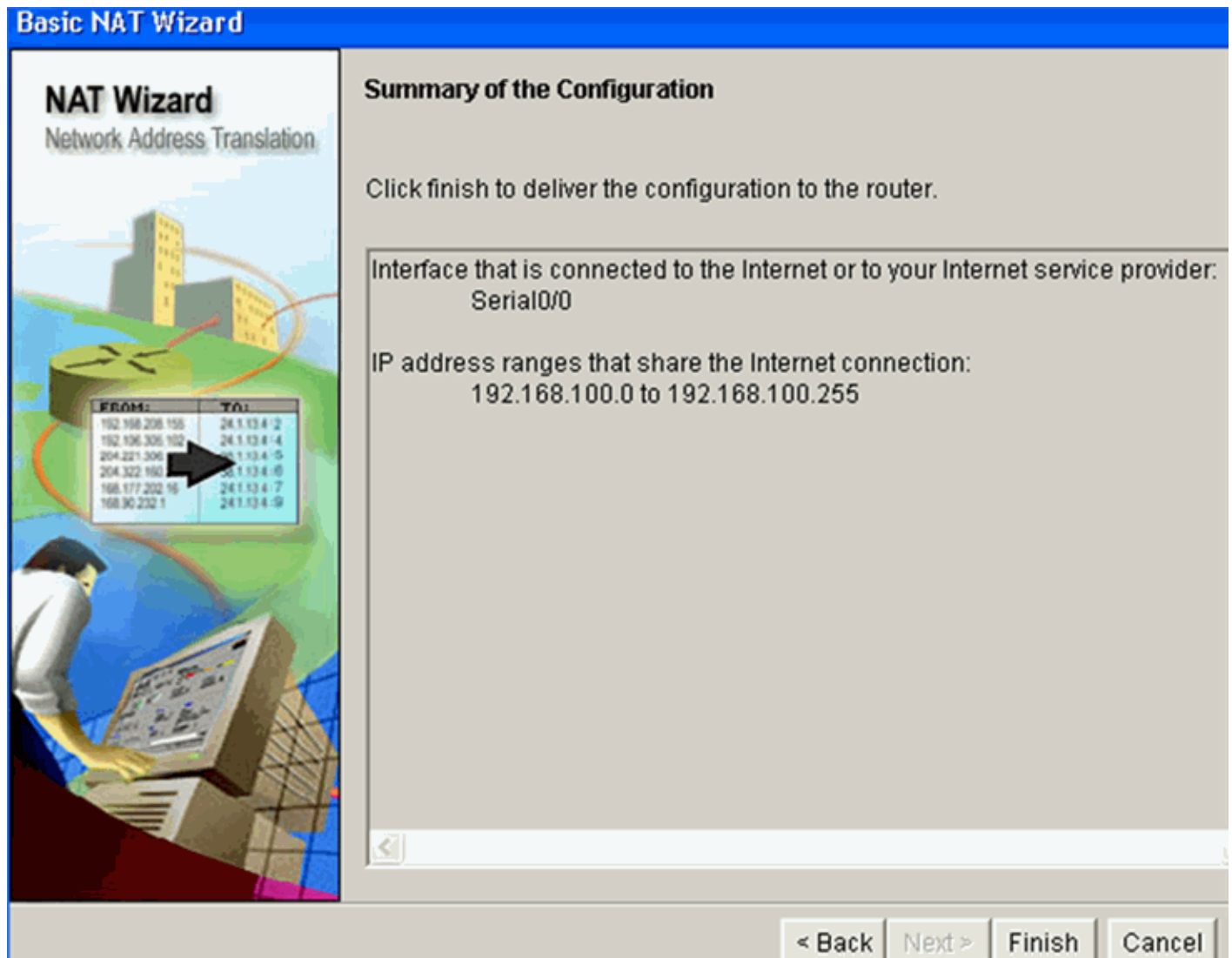
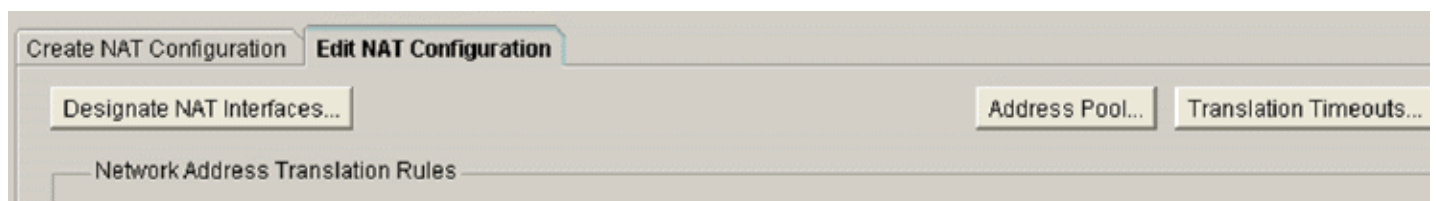


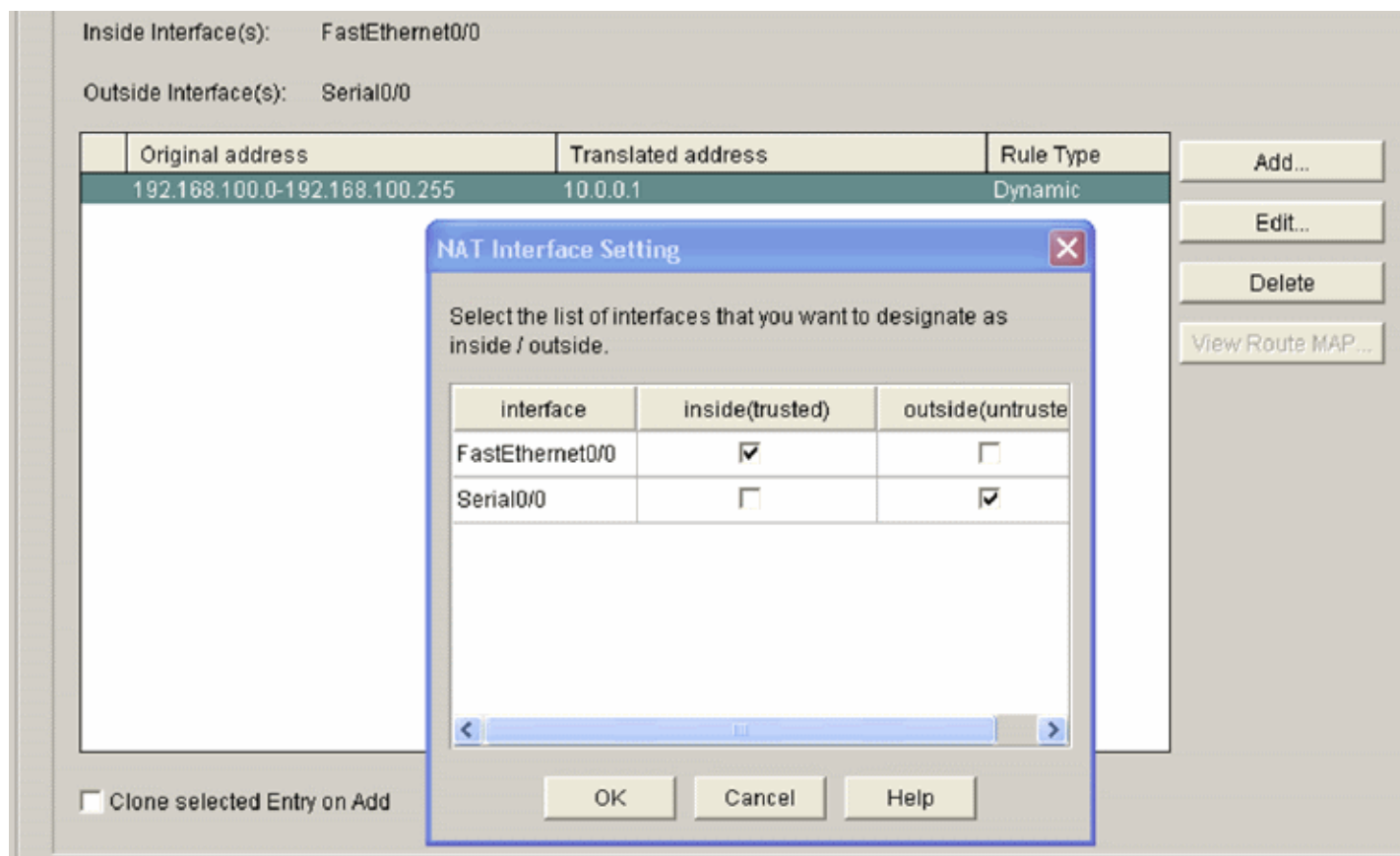
SDM Lab 2 - NAT

You can then confirm the changes by clicking 'finish' on the next screen.



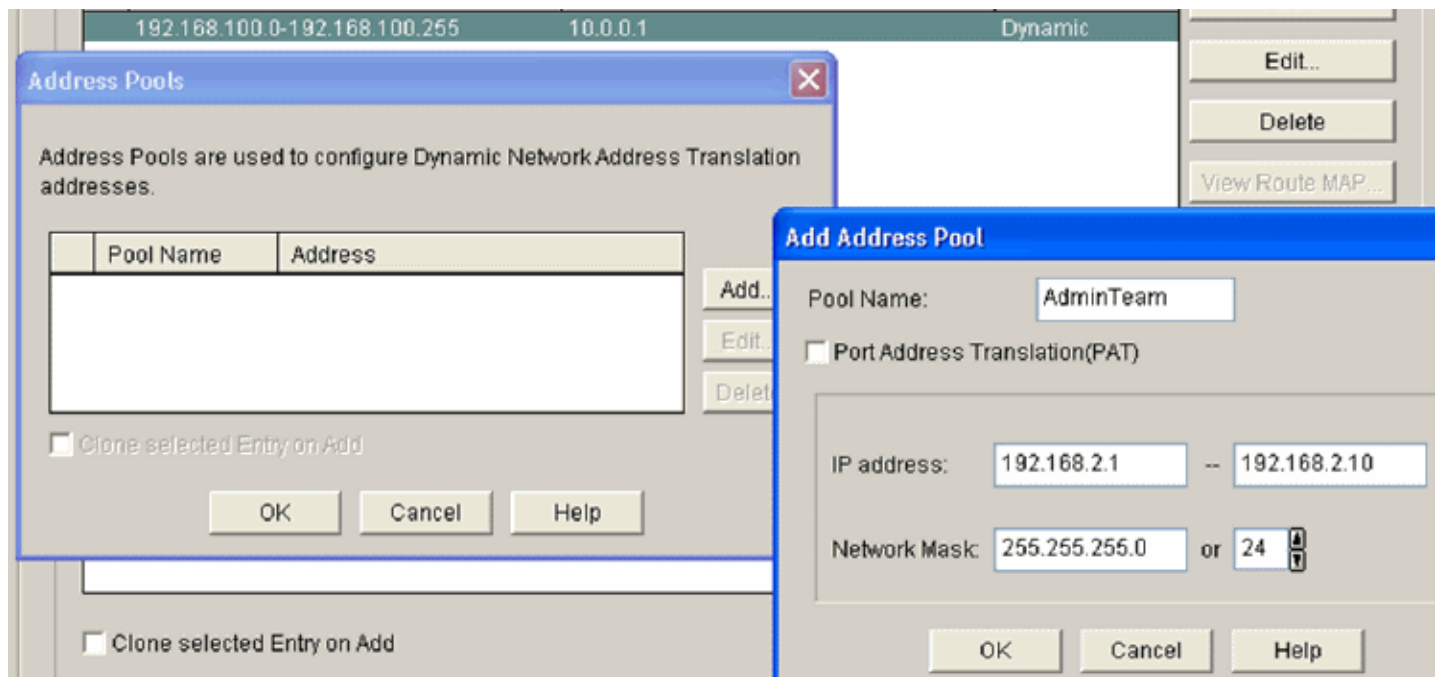
You can now click on the 'Edit NAT Configuration' button and then 'Designate NAT Interfaces' button to see how your interfaces have been allocated.





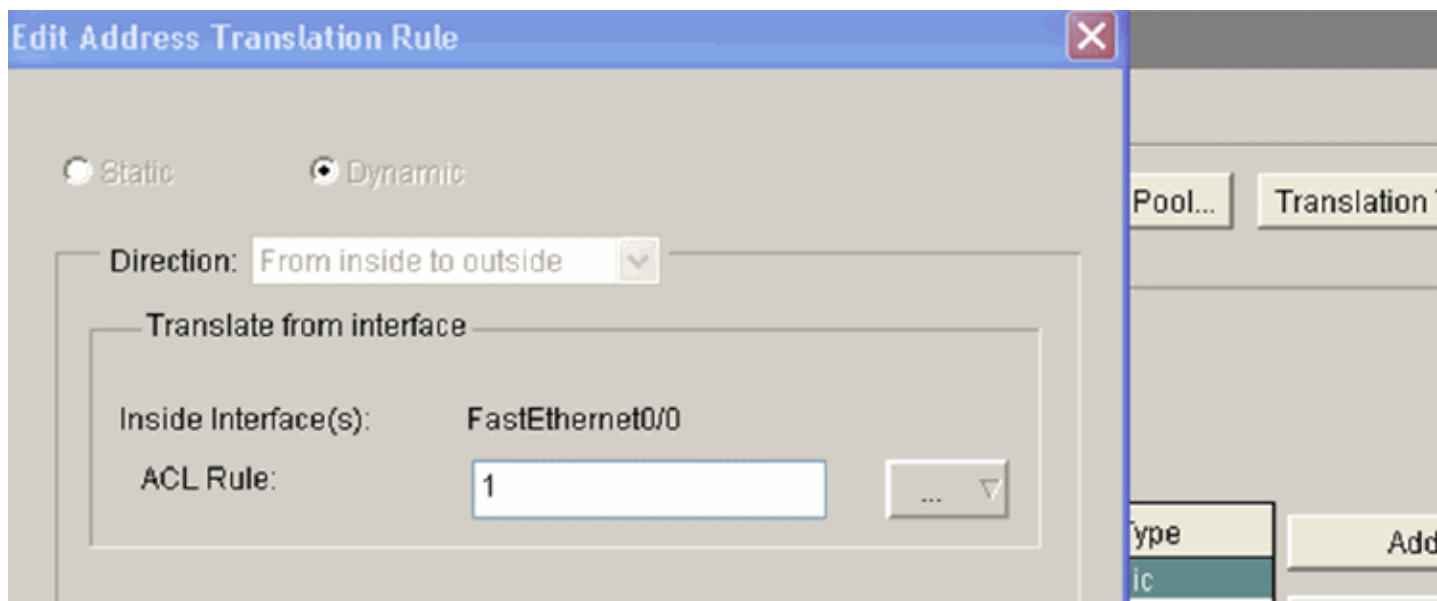
3. We can now add the NAT pool. This is the pool of addresses which will be used for our outside connections. Click on 'Address Pool' at the top right and then 'Add' and then add the pool of addresses you will use to NAT. In this lab we will use 192.168.2.1 to 10.





4. You then need to 'Edit' the NAT configuration once more because, by default, the router will use the IP address of the outside interface and overload it. We want to use our NAT pool 'AdminTeam.'

Click on 'Edit' and then from the drop down list in the 'Translate to Interface' section choose 'address pool' and then in the 'Address Pool' box type 'AdminTeam' making sure that you match the case exactly.

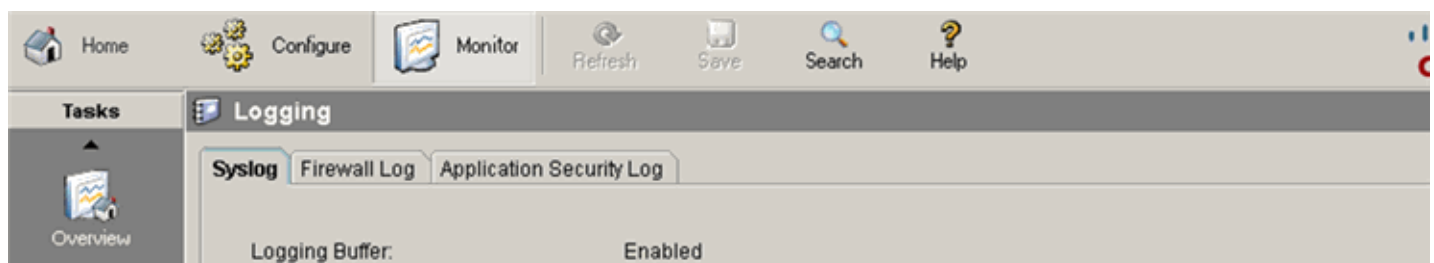


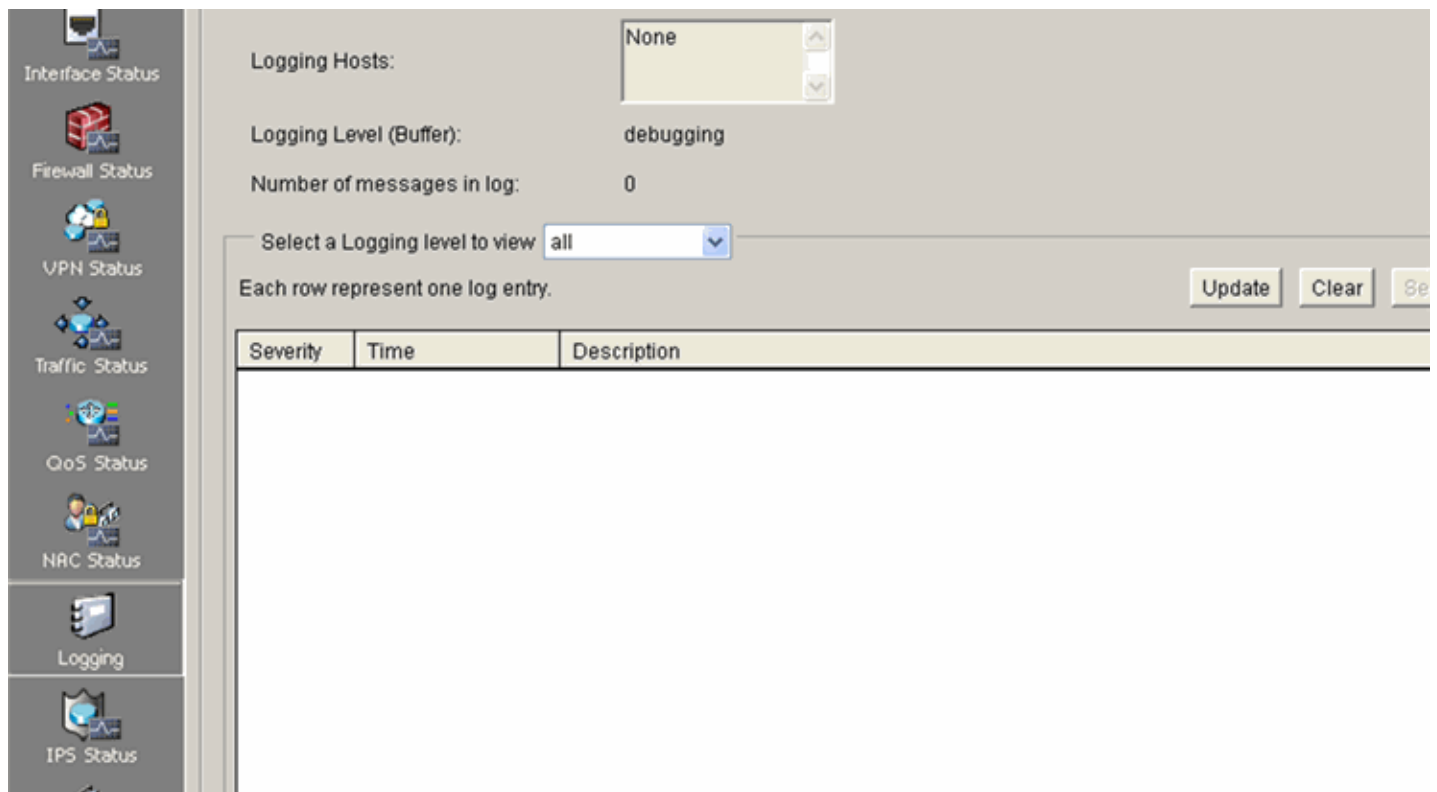
5. If you now view the running config on RouterA you would see the below lines which are the relevant part for our NAT lab:

```
interface FastEthernet0/0
ip address 192.168.100.1 255.255.255.0
ip nat inside
duplex auto
speed auto
interface Serial0/0
ip address 10.0.0.1 255.0.0.0
ip nat outside!
ip nat pool AdminTeam 192.168.2.1 192.168.2.10 netmask 255.255.255.0
ip nat inside source list 1 pool AdminTeam!
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 192.168.100.0 0.0.0.255
```

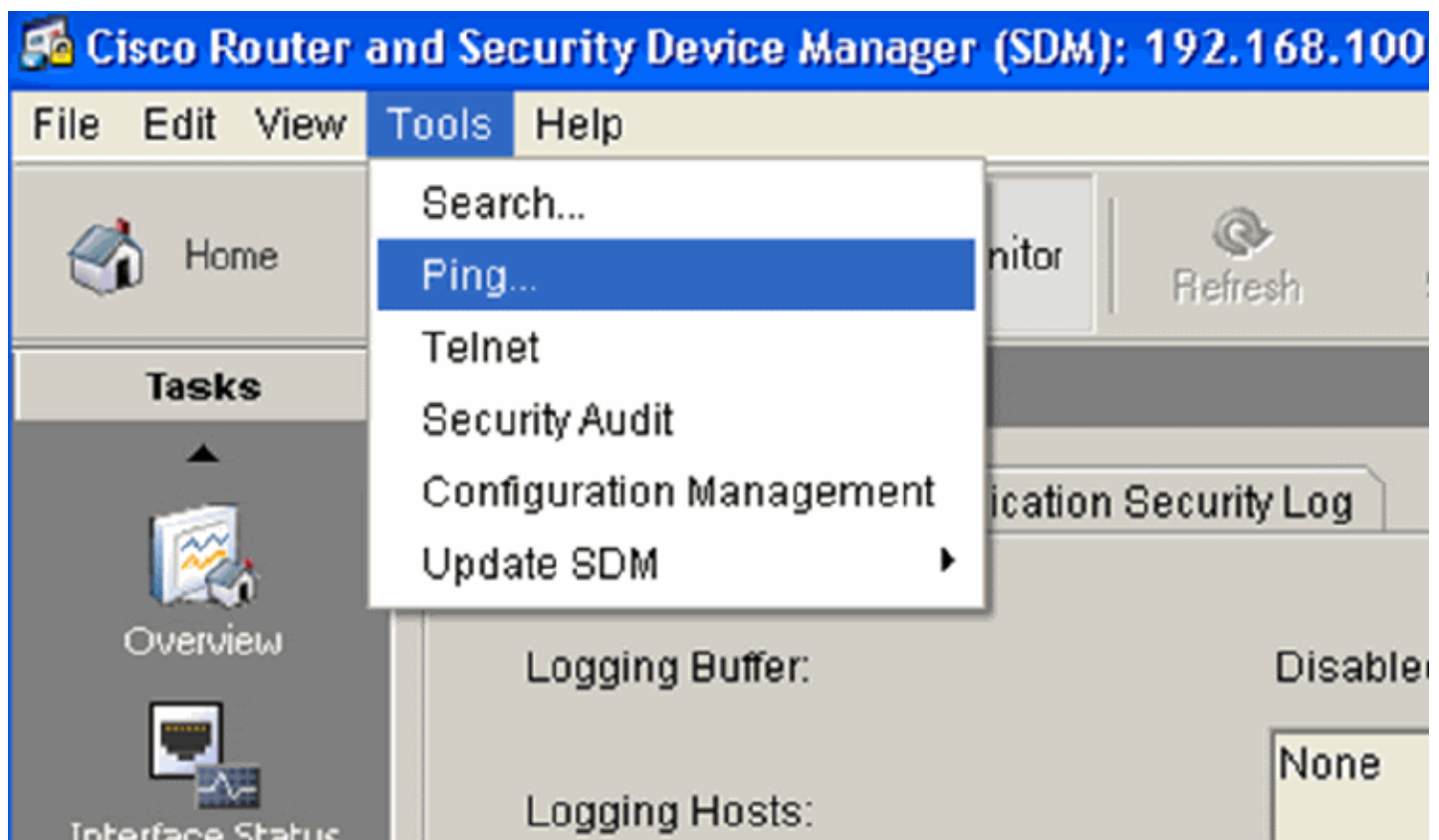
6. We can now monitor the NATting taking place.

Click on 'Monitor' at the top and then 'Logging' along the lower left options. You will want to change the 'Select a logging level to view' to 'all.' If your logging buffer is marked as 'disabled' you can enable it in the 'Configure -- Additional Tasks -- Router Properties -- Logging' area.





And then open the ping tool via the tools menu.



You can source the ping from the Ethernet interface to the serial on RouterA.



* Source:
 Destination:

Sending 5, 100-byte ICMP Echos to 10.0.0.2 timeout is 2 seconds
 !!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57.

(*) Optional Field

7. Now go back to the logging page and press 'update' and you should see the NAT translations taking place.

Logging

Syslog Firewall Log Application Security Log

Logging Buffer: Enabled
 Logging Hosts:
 Logging Level (Buffer): debugging
 Number of messages in log: 10

Select a Logging level to view

Each row represent one log entry.

Severity	Time	Description
debug	Mar 1 02:21:40.870	s=192.168.100.1->192.168.2.1, d=10.0.0.2 [85]
debug	Mar 1 02:21:40.902	s=10.0.0.2, d=192.168.2.1->192.168.100.1 [85]
debug	Mar 1 02:21:40.902	s=192.168.100.1->192.168.2.1, d=10.0.0.2 [86]
debug	Mar 1 02:21:40.934	s=10.0.0.2, d=192.168.2.1->192.168.100.1 [86]
debug	Mar 1 02:21:40.934	s=192.168.100.1->192.168.2.1, d=10.0.0.2 [87]
debug	Mar 1 02:21:40.962	s=10.0.0.2, d=192.168.2.1->192.168.100.1 [87]
debug	Mar 1 02:21:40.966	s=192.168.100.1->192.168.2.1, d=10.0.0.2 [88]
debug	Mar 1 02:21:40.994	s=10.0.0.2, d=192.168.2.1->192.168.100.1 [88]
debug	Mar 1 02:21:40.998	s=192.168.100.1->192.168.2.1, d=10.0.0.2 [89]
debug	Mar 1 02:21:41.026	s=10.0.0.2, d=192.168.2.1->192.168.100.1 [89]

Address 192.168.100.1 (s for source) is translated to 192.168.2.1 (the first address in our pool) and the destination (marked with d) is 10.0.0.2.

I strongly advise you to practise static and dynamic NAT using SDM as well as overloading the serial interface and also using static port mapping. You never know what you will be asked to configure in the exam and so it is best to be prepared for a hard question.

